

















ZARA PRIVACY POLICY

ITX Korea Limited (hereinafter referred to as the “Company” or “We”) duly processes and safely manages personal data in compliance with the Personal Information Protection Act (“PIPA”) and other applicable laws and regulations to protect the freedom and rights of data subjects (hereinafter referred to as “You” or the “data subject”). Accordingly, we establish and disclose this Privacy Policy in order to inform you of the procedures and standards for processing personal data and resolve related grievances in accordance with Article 30 of the PIPA. This Privacy Policy shall be applicable to our use of your personal data, regardless of the channels or means (hereinafter referred to as the “Platform”) that you use to interact with www.zara.com.

[Labeling of Major Categories of Personal Information Processing]			
Collected Items 	Processed Items 	Purpose 	Behavioral Information 
<ul style="list-style-type: none"> Email address, name, address/zip code, phone number, etc. 	<ul style="list-style-type: none"> To manage your registration, etc. 	<ul style="list-style-type: none"> Right to accept or refuse collection 	
Overseas Transfer 	Outsourcing 	Retention Period 	Destruction 
<ul style="list-style-type: none"> 2 entities including Inditex S.A. Platform operation 	<ul style="list-style-type: none"> 10 entities including Hanjin Payment/ delivery, etc. 	<ul style="list-style-type: none"> Retained and destroyed by the time specified in this Privacy Policy, such as when membership is withdrawn or by the time specified in applicable laws 	
Your Rights and Obligations 	Measures to Ensure Safety 	Amendment of Privacy Policy 	Legal Representative 
<ul style="list-style-type: none"> Right to access, correct, delete 	<ul style="list-style-type: none"> Encryption measures, etc. 	<ul style="list-style-type: none"> Previous policies disclosed 	<ul style="list-style-type: none"> Represent minors
Data Protection Officer 	Grievance Handling Department 	Request for Access 	Authority 
<ul style="list-style-type: none"> Data Protection Team / dataprotection@zara.com / “My Account” 			<ul style="list-style-type: none"> www.kopico.go.kr

1. PURPOSE OF COLLECTION, COLLECTED ITEMS AND RETENTION PERIOD

(a) Items of personal data processed without the consent of the data subject

We process your personal data without your consent as follows:

Legal Basis	Category	Purpose of Collection	Collected Items	Period of Retention and Use
Article 15(1)(iv) (Performance of Contract) of the PIPA	Membership Service	Shipping products and processing returns	phone number, address	Until your account is terminated
Article 15(1)(iv) (Performance of Contract) of the PIPA	A/S consultation on products	Handling of complaints and consultation regarding transactions	name, phone number, purchase history	3 years (Article 6 of the Act on the Consumer Protection in Electronic Commerce)
Article 15(1)(iv) (Performance of Contract) of the PIPA	Processing orders and payments	Processing orders and payments	order number, payment method	5 years (Article 6 of the Act on the Consumer Protection in Electronic Commerce)

(b) Items of personal data processed upon the consent of the data subject

We process your personal data upon your consent as follows, in accordance with Article 15(1)(i) and Article 22(1)(vii) of the PIPA:

Purpose of Collection	Collected Items	Period of Retention and Use
To manage your registration as user of the Platform, sales of goods, provision of service, handling of inquiries/requests and prevention of fraudulent use.	Email address, password, name, phone number	Until your account is terminated*
To introduce new products and services or perform promotional actions.	Email address, field of interest	Until you unsubscribe the Newsletter

* However, if there is an ongoing investigation due to a violation of applicable laws and regulations, until the completion of the investigation; if there is any remaining creditor-debtor relationship arising from the use of the Platform, until such creditor-debtor relationship is settled.

(c) In the process of using the service, the following information can be automatically generated and collected: your location data, device identification number, type of browser, IP address from which payment is made, preference related to the historic purchase and browsing history, and advertising ID.

(d) We provide Social Media log in service and receive personal data from Social Media during the process.

(e) Certain data will be kept longer than the period mentioned above, as stipulated by relevant laws as follows:

- (i) Under the Protection of Communication Secrets Act:
 - Service usage record, access log, IP information: 3 months
- (ii) Under the Act on the Consumer Protection in E-commerce:
 - Records related to marks and advertisements: 6 months
 - Records related to cancellation of contracts or subscription, etc.: 5 years
 - Records related to payment for and supply of goods, etc.: 5 years
 - Records related to resolution of consumer complaints or disputes: 3 years

2. PROCEDURE AND METHOD OF PERSONAL DATA DESTRUCTION

(a) We destroy the personal data when it becomes unnecessary, such as when the retention period has expired or the purpose of processing has been fulfilled.

(b) However, if the personal data needs to be retained in accordance with relevant laws despite the expiration of retention period or achievement of processing purposes, the personal data will be preserved separately.

* The item and legal basis of the personal data preserved under other laws can be found in the “1. Purpose of Collection, Collected Items and Retention Period” section.

(c) Personal data in the form of electronic files is destroyed in a non-reversible manner, and personal data written and stored in paper documents is shredded or incinerated.

3. THIRD PARTY PROVISIONS OF PERSONAL DATA

We may provide personal data to related authorities without the consent of the data subject as follows, in cases of emergencies such as disasters, infectious diseases, accidents or events that poses an imminent danger to life or body, or imminent loss of property. In such cases, we will provide only the minimum extent of personal data necessary for these purposes and will not provide it for any other purpose.

Category	Legal Basis	Recipient	Provided Items
Disaster Countermeasure	Article 74-3 (Request for Provision of Information) of the Framework Act On The Management Of Disasters And Safety	Central Countermeasure Headquarters or local countermeasure headquarters	<ul style="list-style-type: none"> ▪ name, address, phone number (including mobile phone number) ▪ Information for identifying movement routes and searching, rescuing: Information collected through CCTV
Control and prevention of infectious disease	Article 76-2 (Request for Provision of Information and Verification of Information) of the Infectious Disease Control And	Disease Control and Prevention Agency or Si·Do	<ul style="list-style-type: none"> ▪ name, address, phone number (including mobile phone number) ▪ Information for identifying movement routes: Video information collected through visual data processing device under the PIPA

	Prevention Act		
Protection of persons at suicide risk	Article 19-3 (Requests for Provision of Information to Rescue People in Need of Emergency Rescue) of the Act On The Prevention Of Suicide And The Creation Of Culture Of Respect For Life	Police agency, Coast guard agency, Fire service agency,	• name of persons in need of emergency rescue, address, phone number, email address
Processing personal data of persons involved in crimes such as kidnapping and imprisonment	Article 18(2)(vii) (Restriction on Repurposing Personal Information and Provision Thereof) of the PIPA	Police agency	• Video information such as CCTV data

4. OUTSOURCING OF PERSONAL DATA PROCESSING

(a) For effective handling of duties relating to personal data, we outsource the processing of personal data to the following entities:

(i) Status of Outsourcing

Name of the outsourcee	Details of the outsourced work
Zara Retail Korea Co., Ltd.	Customer Service related to order, shipment, return, etc.
NHNKCP Corp.	Payment Gateway
NICEPAY Co., Ltd.	Payment Gateway
Maersk Contract Logistics Korea Limited.	Managing delivery and return
CJ Logistics Corporation	Delivery
Lotte Global Logistics Co., Ltd.	Delivery
Hanjin Transportation Co., Ltd.	Delivery
Logen Co., Ltd.	Delivery
Herewego Co., Ltd.	Delivery

(ii) Status of Sub-contracting

Name of the outsourcee	Status of sub-contracting
NHNKCP Corp.	See Privacy Policy
NICEPAY Co., Ltd.	See Privacy Policy

CJ Logistics Corporation	See Privacy Policy
Lotte Global Logistics Co., Ltd.	See Privacy Policy
Hanjin Transportation Co., Ltd.	See Privacy Policy
Logen Co., Ltd.	See Privacy Policy
Herewego Co., Ltd.	See Privacy Policy
Link Mobility	Texting Service
Concentrix Service Korea	Customer Care Service

(b) When entering into contracts with an outsourcee, we specify the following in documents as contracts in accordance with Article 26 of the PIPA: prohibition of personal data processing for any purpose other than the performance of outsourced work, technical and managerial measures for protecting personal data, restrictions on sub-contracting, management and supervision of the outsourcee, and matters regarding liabilities for damages. We supervise whether the outsourcee processes your personal data securely.

(c) In accordance with Article 26(6) of the PIPA, the outsourcee obtains our consent when they sub-contract the processing of personal data to a third party.

(d) We will inform you any changes of this section without delay via amending this Privacy Policy.

(e) The overseas transfer of personal data is described in the “5. Overseas Transfer of Personal Data” section.

5. OVERSEAS TRANSFER OF PERSONAL DATA

We outsource the processing of personal data we collected to the following overseas entities, in accordance with Article 28-8(1)(iii)(a)(Overseas Transfer of Personal Data for Contract Performance) of the PIPA. If you refuse the overseas transfer, you will not be able to use our service. Should you wish to refuse the transfer, you can withdraw your membership from the platform or request withdrawal of membership through the customer center.

Transferred Items	Transfer red Country	Transfer Date and Method	Recipient	Purpose of use	Period of Retention and Use
Email address, password, name, address/ZIP code, phone number, payment method, the location data, the device identification number, type of browser, IP address from which payment is made, preference related to the historic purchase and	Spain, Ireland	Personal data is collected at the time of use of the service via website/app and then transferred via telecommunications network or other electronic or paper-based means	Industria de Diseño Textil, S.A. (Inditex, S.A) (dataprotection@zara.com)	Corporate policies fulfillment and compliance	Same as the retention period set forth in this Privacy Policy

browsing history, advertising ID					
Email address, password, name, address/ZIP code, phone number, payment method, the location data, the device identification number, type of browser, IP address from which payment is made, preference related to the historic purchase and browsing history, and advertising ID	Netherlands	Personal data is collected at the time of use of the service via website/app and then transferred via telecommunications network or other electronic or paper-based means	ITX Merken B.V (dataprotection@zara.com)	Technology development, e-commerce platform support and Customer Service	Same as the retention period set forth in this Privacy Policy

6. MEASURES TO ENSURE THE SECURITY OF DATA

We apply the following security measures to protect your data:

1. Conduct regular audits

To ensure the security of personal data, we conduct regular self-audits.

2. Minimizing and training of employees who process personal data

We take measures to manage personal data by designating a limited number of employees with access to personal data.

3. Establishment of Internal Management Plan

We have established and implemented an Internal Management Plan to process personal data securely.

4. Technical measures against cyberattack

We install, periodically update and inspect security programs to prevent leakage or damage of personal data caused by hacking, computer viruses, etc. We also keep our systems in facilities where access from outside is restricted.

5. Encryption of personal data

Your password is encrypted for storage and management. In addition, we apply security measures to protect other important data.

6. Storage of access records and prevention of forgery.

We keep records of access to personal information processing system according to relevant laws and regulations. Also, we implement security measures to prevent forgery, theft or loss of such records.

7. Restricting access to personal data

We implement necessary measures to control access to personal data by granting, changing and cancelling access rights to the personal data processing database system. We use an intrusion prevention system to control unauthorized access from outside.

8. Use of lock for document security

We keep documents or auxiliary storage media that contains personal data in a safe and locked place.

7. INSTALLATION, OPERATION AND REFUSAL OF AUTOMATIC PERSONAL DATA COLLECTION DEVICES

- (a) We use “cookies” which store and retrieve data periodically, to provide you with personalized service and convenience.
- (b) A cookie is a small piece of data that a server (http), used to operate the website, sends to your browser, and is stored on your PC or mobile device.
- (c) You can choose to allow or deny cookies by adjusting the web browser option. However, if you refuse storing cookies, you may have difficulties in using customized services.

8. COLLECTION, USE AND REFUSAL OF BEHAVIORAL INFORMATION

- (a) To provide optimized, personalized services and benefits as well as personalized online ads during your service usage, we collect and use behavioral information through cookies, without identifying individuals.
- (b) To provide services such as personalized online ads, we collect and use behavioral information via an automatic personal data collection device installed on website and app operated by a third party.
- (c) We collect only the minimum behavioral information necessary for the personalized services and benefits. We do not collect any sensitive behavioral information that may infringe upon any individual's rights, interests, or privacy, such as ideology, belief, educational background, medical history.
- (d) You may allow or block all personalized online ads by changing the cookies settings on your web browser. However, modifying the cookies settings may limit you from using certain services as automatic website log-in.
- (e) We collect and use advertising IDs for personalized ads in our Android App. You can allow or block personalized ads in App by changing the settings on your mobile device.
- (f) You may contact the department in charge of personal data protection to inquire about any questions regarding behavioral information, exercising your right of refusal, and filing damage.

9. RIGHTS AND OBLIGATIONS OF DATA SUBJECT AND LEGAL REPRESENTATIVE

- (a) You may exercise the right to access, rectify, erase, limit or request withdrawal of your personal data processing at any time. If you are a minor aged 14 or above, you may exercise your rights either directly or through your legal representative.
- (b) You may exercise the rights in writing, via e-mail, etc., as outlined in Article 41(1) of the Enforcement Decree of the PIPA. We will take actions upon your request at any time without delay.
 - You can access, modify, or erase personal data directly in the “Account > Profile” section of the website at any time.
 - You can withdraw consent for the collection and use of personal data in the “Account > Profile > Delete Account” section at any time.
- (c) You may also exercise your rights under this section through a legal representative or an attorney. In such cases, you shall submit a power of attorney by using the Attached Form No.11 under ‘Notice

on Personal Information Processing Method’.

(d) Your right to request access or limitation of processing personal data may be restricted in accordance with Article 35(4) and Article 37(2) of the PIPA.

(e) You cannot request rectification or erasure of personal data if we are obligated to collect such data under relevant laws.

(f) We verify whether the person requested to exercise the rights is the subject of such rights or a legitimate representative.

(g) You may exercise your rights by contacting the department in charge of personal data protection. We will make every effort to promptly process your exercise of rights.

10. DEPARTMENT IN CHARGE OF PERSONAL DATA PROTECTION

(a) We appointed a Data Protection Officer (“DPO”) and are operating a department in charge of personal data protection as follows. They are tasked with overall responsibility for processing personal data, and handle complaints and damage relief of data subjects related to personal data processing.

- Data Protection Department
TEL: 080-479-0880
Email: dataprotection@zara.com

(b) You may contact the department in charge of personal data protection for all inquiries related to personal data protection, complaints, and damage relief, arising while using our service. We will respond and handle your inquiries without delay.

11. METHODS FOR REMEDYING INFRINGEMENT OF RIGHTS OF DATA SUBJECTS

(a) We inform you that you have the right to file a claim before the responsible data protection regulatory authority.

- Personal Information Dispute Mediation Committee (www.kopico.go.kr / 1833-6972)
- KISA Personal Information Infringement Reporting Center (privacy.kisa.or.kr / 118)
- Supreme Prosecutors’ Office (www.spo.go.kr / 1301)
- National Police Agency (ecrm.cyber.go.kr / 182)

(b) We strive to secure the right to self-determination of personal data for data subjects, and to consult and remedy damage caused by infringement of personal data. If you need to report or seek consultation, please contact to the department in charge of personal data protection.

12. AMENDMENT OF PRIVACY POLICY

(a) This Privacy Policy is entering into force on August 20, 2024.

(b) The previous version of this Privacy Policy is available at the link below:

- Effective before [August 20, 2024](#)
- Effective before [May 24, 2024](#)
- Effective before [August 1, 2023](#)
- Effective before [May 1, 2023](#)

- Effective before [May 2, 2022](#)
- Effective before [August 2, 2021](#)
- Effective before [May 14, 2021](#)